Deutscher Bundestag **Drucksache 19/11755**

19. Wahlperiode 18.07.2019

Kleine Anfrage

der Abgeordneten Dr. Konstantin von Notz, Agnieszka Brugger, Tabea Rößner, Dieter Janecek, Dr. Franziska Brantner, Dr. Tobias Lindner, Luise Amtsberg, Canan Bayram, Kai Gehring, Britta Haßelmann, Katja Keul, Monika Lazar, Dr. Irene Mihalic, Filiz Polat, Dr. Manuela Rottmann, Dr. Frithjof Schmidt und der Fraktion BÜNDNIS 90/DIE GRÜNEN

IT-Sicherheit durch mehr Transparenz und Standardisierung bei Zählweisen und Klassifizierungen von Angriffen

Zur Erlangung eines präzisen und faktenbasierten Lagebildes und zu den Grundlagen guten Regierens auch im Feld der IT-Sicherheit gehört es nach Ansicht der Fragesteller, möglichst eindeutige, transparente und nachvollziehbare Kennzahlen zur Nachzeichnung der Entwicklung im Bereich von IT-Angriffen zu erreichen. Nur auf der Grundlage faktenbasierter und nachvollziehbarer Darstellungen kann auch der Deutsche Bundestag zu problem- und sachbezogenen Diskussionen hinsichtlich seiner Kontroll- und Regulierungsaufträge in dieser für die Sicherheit der Bevölkerung zentralen Thematik gelangen.

Auf die Notwendigkeit klarer Definitionen und Zuständigkeiten bei der Abwehr von IT-Angriffen wurde wiederholt, auch in parlamentarischen Initiativen (vgl. beispielsweise Forderung h des Antrags der Fraktion BÜNDNIS 90/DIE GRÜNEN „IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern“ auf Bundestagsdrucksache 19/1328) hingewiesen. An der gängigen Praxis der pauschalisierenden Veröffentlichung von zum Teil extrem hohen oder auch niedrigen Zahlen ohne nähere Erläuterung von deren Zustandekommen (vgl. beispielsweise die Meldung der Bundesregierung, www.heise.de/newsticker/meldung/Ueber-47-Millionen-IT-Angriffe-auf-die-Bundeswehr-im-Jahr-2016-3595632.html) bestehen mit Blick auf die Notwendigkeit einer differenzierten und zutreffenden Einschätzung dieser komplexen Risiken durch die Öffentlichkeit aus Sicht der Fragesteller erhebliche Zweifel (Hinweise dazu etwa unter www.defenseone.com/ideas/2018/09/cyberspace-governments-dont-know-how-count/151629/?oref=d-river).

Wir fragen deshalb die Bundesregierung:

1. Welche Stellen sind innerhalb der Bundesregierung und der ihr nachgeordneten Behörden mit der Klassifizierung und der Abwehr von IT-Angriffen beschäftigt (bitte im Einzelnen aufschlüsseln)?
2. Welches Bundesministerium hat eine federführende bzw. koordinierende Funktion bei der Klassifizierung und der Abwehr von IT-Angriffen, und auf welchem Weg findet die Koordination zwischen den verschiedenen, mit der Thematik betreuten Bundesministerien statt?

3. Welche Bundesministerien und nachgeordneten Bundesbehörden veröffentlichten (in Pressestatements der Hausleitungen usw.) in den zurückliegenden fünf Jahren eigene Zahlen zu Angriffen auf ihre eigenen IT-Systeme, IT-Netze, Infrastrukturen oder die IT-Systeme Dritter bzw. auf die IT-Infrastruktur der Bundesregierung insgesamt (bitte im Einzelnen auflisten)?
4. In wie vielen dieser Fälle erfolgten diese Veröffentlichungen auf Anweisung oder in Absprache mit einem der Bundesministerien (bitte entsprechend unterscheiden, welche, und Hintergrund darlegen)?
5. Welche Gefahrenstufen unterscheidet die Bundesregierung für das Vorliegen von Zugriffsversuchen, wie sind diese im Einzelnen definiert und kann die Bundesregierung eine für die Ressorts unterscheidbare Aufschlüsselung der jeweiligen Jahresstatistik nach Gefahrenstufen, wie etwa eine Antwort der Bundesregierung auf eine Frage des Abgeordneten Alexander Graf Lambsdorff (vgl. Bundestagsdrucksache 19/2922, Frage 87, S. 65) nach Ansicht der Fragesteller suggeriert, vorlegen?
6. In welcher Hinsicht haben sich konkret zwischen 2016 und 2017 aufgrund welcher Überlegungen und Vorgänge die Vorgaben für die statistische Zählweise als auch die Bewertungen für die Gefahrenstufe verändert (vgl. ebd.)?
7. Hält die Bundesregierung die derzeitig genutzten Definitionen für ausreichend ausdifferenziert, um der Problematik angemessen zu begegnen?
8. Über welche Zahlen verfügt die Bundesregierung bezüglich Angriffen der Gefahrenstufe sog. Advanced Persistent Threats (APT) auf Bundesministerien oder Behörden in ihrem Geschäftsbereich (bitte im Einzelnen aufschlüsseln)?
9. Besteht für die Erkennung, Zählung und deren Definition bzw. Klassifizierung als IT-Angriff eine übergeordnete und/oder abgestimmte, für alle Bundesministerien und Bundesbehörden geltende Vorgehensweise oder gar Erlasslage?

   Wenn ja, welche konkret, und welche Informationen sind zu jedem Angriff aufzuzeichnen?

   Wenn nein, warum nicht?
10. Besteht aus Sicht der Bundesregierung eine (beispielsweise durch eine solche Erlasslage ermöglichte) Vergleichbarkeit zwischen Angriffen (Quantität und Qualität) auf einzelne Bundesministerien und Bundesbehörden?
11. Besteht für die Erkennung, Zählung und Definition bzw. Klassifizierung als IT-Angriff eine zwischen einzelnen oder mehreren Behörden des Bundes und der Länder abgestimmte Vorgehensweise, und wenn nein, warum nicht?
12. Sollte es die in Frage 9 erfragte, übergeordnete und/oder abgestimmte, für alle Bundesbehörden geltende Vorgehensweise oder gar Erlasslage für die Erkennung, Zählung und deren Definition bzw. Klassifizierung als IT-Angriff nicht geben, gibt es zumindest für die innerhalb des Cyberabwehrzentrums (CAZ) zusammenarbeitenden Bundesministerien und Behörden hinsichtlich IT-Angriffen einheitliche Definitionen?

    Falls nicht, was hat die Bundesregierung bislang unternommen, um die unterschiedlichen Definitionen anzugleichen?
13. Besteht für die Erkennung, Zählung und Definition bzw. Klassifizierung als IT-Angriff eine zwischen einzelnen oder mehreren Behörden europäischer Mitgliedstaaten oder in Organisationen wie der NATO abgestimmte Vorgehensweise, und wenn nein, warum nicht?

14. Wird die Bundesregierung sich für eine stärkere Klassifizierung und/oder Standardisierung einsetzen?

    Falls ja, welche Pläne gibt es hierfür konkret?

    Falls nein, warum nicht, und wird hierfür keine Notwendigkeit gesehen?

15. Hat es zwischen Behörden des Bundes jemals eine Diskussion und/oder eine Verständigung über eine entsprechende Matrix im Umgang mit der Erkennung, Definition bzw. Klassifizierung und der Zählung von IT-Angriffen gegeben, und wenn ja, wann, in welchem Rahmen (etwa im CAZ, während einer Sitzung der IMK usw.), welchen Inhalts und mit welchem Ergebnis (ggf. bitte entsprechende Handlungsanweisungen bzw. Erlasse etc. beifügen)?

16. Plant die Bundesregierung eine entsprechende übergreifende oder zumindest für einzelne Behörden vorzunehmende Vereinheitlichung und/oder Standardisierung in der Klassifizierung und Zählung von IT-Angriffen, und wenn nein, warum nicht?

17. Welche Formen von IT-Vorfällen (z. B. Pings, Port-Scans, E-Mails mit Schadprogrammen, Vireninfektionen etc.) werden in den unterschiedlichen Behörden für die Zählung berücksichtigt (bitte im Einzelnen aufzählen), und welche Risikoerwägungen liegen diesen Einordnungen jeweils zugrunde?

18. Handelt es sich bislang im Schwerpunkt allein um die Zählung von durch Anti-Viren-Schutzmaßnahmen erfasste Schadprogramme (vgl. etwa BSI-Bericht von 2017 www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4), und wie werden diese Schadprogramme gezählt (z. B. Zählung je tatsächlich oder potentiell erreichtem E-Mail-Account oder Zählung nur ein Mal pro aufgefundenem, unterscheidbarem Schadprogramm etc.)?

19. Zählen Spam-Mails und/oder Phishing-Mails nach wie vor als (einzeln zu erfassende) IT-Angriffe, und wenn ja, bei welchen Behörden?

20. Zählen groß angelegte Angriffe, die über lange Zeiträume (Wochen oder Monate) durchgeführt werden, als einzelne IT-Angriffe, oder werden diese mehrfach erfasst?

    Wie wurde beispielsweise der Angriff auf die Netze des Deutschen Bundestages in der ersten Hälfte des Jahres 2015 gezählt?

21. In welcher Form werden durch IT-Angriffe ausgelöste Schäden und Beeinträchtigungen ermittelt und erfasst?

22. Bestehen einheitliche Regeln dazu, in welcher Form, welchem Umfang und innerhalb welcher Frist die von IT-Angriffen betroffenen Bundesbehörden über diese in Kenntnis gesetzt werden müssen?

23. Teilt die Bundesregierung die Ansicht der Fragesteller, dass Begrifflichkeiten wie „Cyberangriff/Cyberattacke“ zu unspezifisch sind, um ein genaues Lagebild als Grundlage für Abwehrmaßnahmen etc. zu bekommen?

24. Hat die Bundesregierung eine Position zur Frage, ob die Stärkung der IT-Sicherheit eine zentrale Bedingung für das Gelingen der gesellschaftlichen Gestaltung der Digitalisierung, für die Schaffung von Vertrauen in digitale Angebote und Infrastrukturen, für den Erhalt von Freiheit sowie für die Sicherung von Frieden ist und es bezüglich der Stärkung der IT-Sicherheit, der Zusammenarbeit der involvierten Bundesministerien und Behörden sowie der Härtung digitaler Infrastrukturen erheblicher weiterer Anstrengungen bedarf, um der verfassungsrechtlich gebotenen Schutzverantwortung für die Vertraulichkeit und Integrität informationstechnischer Systeme und dem Grundrecht auf Privatheit der Kommunikation gerecht zu werden?

    Wenn nein, warum nicht?

25. Wie ist der derzeitige Stand der Erarbeitung des seit langem angekündigten sogenannten IT-Sicherheitsgesetzes 2.0, und wann wird die Bundesregierung den Gesetzentwurf dem Deutschen Bundestag zur parlamentarischen Beratung vorlegen?

26. Wird die Frage der Erfassung und Klassifizierung von IT-Angriffen im „IT-Sicherheitsgesetz 2.0“ eine Rolle spielen?

27. Gibt es von Seiten der Bundesregierung Überlegungen, die Zuständigkeit für die IT-Sicherheit aus dem Bundesministerium des Innern, für Bau und Heimat herauszulösen und einem anderen Ressort zu übertragen?

    Falls ja, welchem?

    Falls nein, warum nicht?

28. Gibt es von Seiten der Bundesregierung Überlegungen, die Zusammenarbeit im Cyberabwehrzentrum (CAZ) auf eine neue rechtliche Grundlage zu stellen und personell auszubauen?

    Wenn ja, wie konkret?

    Falls nicht, wird die bisherige Form der Zusammenarbeit und der rechtlichen Grundlagen sowie der personellen Ausstattung als gut bewertet?

29. Ist das Cyberabwehrzentrum (CAZ) aktuell rund um die Uhr besetzt und hinsichtlich anwesender Personen arbeitsfähig?

    Falls nein, zu welchen Zeiten ist das CAZ besetzt?

30. Plant die Bundesregierung, das Cyberabwehrzentrum (CAZ) mit einem Koordinator auszustatten, der im Falle eines möglichen Angriffs die Zuständigkeiten der Behörden koordiniert, wie dies der Inspekteur Cyber- und Informationsraum, Generalleutnant Ludwig Leinhos angeregt hatte (vgl.: www.tah.de/welt/afp-news-single/cyber-inspekteur-brauchen-koordinator-im-nationalen-cyber-abwehrzentrum.html)?

31. Welche Aufgaben sollen der Bundeswehr in Zukunft im Rahmen des Cyberabwehrzentrum (CAZ) zufallen?

32. Gibt es von Seiten der Bundesregierung Überlegungen, das Bundesamt für Sicherheit in der Informationstechnik bzw. Teile davon, angesichts der nach Ansicht der Fragesteller immer wieder auftretenden Interessenkonflikte, unabhängig zu stellen, auch, um es in seiner Beratungsfunktion gegenüber Bürgerinnen und Bürgern wie Unternehmen zu stärken?

    Wenn nein, warum nicht?

33. Welche Stelle koordiniert aktuell die notwendige Gesamtbeobachtung hybrider Bedrohungen (hybrid threats), führt die Erkenntnisse zusammen und berichtet dazu innerhalb der Bundesregierung?

34. Gibt es von Seiten der Bundesregierung Überlegungen, neue Zuständigkeiten für die systematische Beobachtung hybrider Bedrohungen zu schaffen, um so mögliche Angriffe, insbesondere auf zivile und für das staatliche Wohl relevante digitale sowie kritische Infrastrukturen, identifizieren und abwehren zu können?

    Falls ja, welche konkret?

    Falls nein, werden die derzeit zur Verfügung stehenden Strukturen als ausreichend betrachtet?

35. Gibt es von Seiten der Bundesregierung Überlegungen, eine eigenständige, fachlich unabhängige Organisationseinheit zur Bewertung einer etwaigen Zurechenbarkeit von Angriffen (Attribution) zu schaffen?

    Falls ja, welche konkret?

    Falls nicht, warum wird dies als nicht notwendig erachtet?

36. Hält die Bundesregierung an ihren Plänen, eine gesetzliche Grundlage zur Ermöglichung digitaler Gegenschläge, sogenannter Hackbacks, fest, und wer soll nach den bisherigen Plänen der Bundesregierung auf welcher Rechtsgrundlage die politische wie rechtliche Verantwortung für derartige Angriffe übernehmen?

37. Welche konkreten Pläne und Überlegungen haben die Bundesregierung oder einzelne Bundesministerien hierzu in den vergangenen zwölf Monaten angestellt, welche Treffen haben hierzu zwischen verschiedenen Bundesministerien stattgefunden, welche Papiere wurden hierzu erarbeitet, welche Gutachten, beispielsweise zu verfassungs-, europa- und/oder völkerrechtlichen Fragen, bei wem in Auftrag gegeben und welche „Stufenpläne“ erstellt (vgl. www.tagesschau.de/investigativ/seehofer-cyberabwehr-103.html)?

38. Gibt es nach Kenntnis der Bundesregierung eine im Koalitionsvertrag zwischen CDU, CSU und SPD festgehaltene, diesbezügliche Vereinbarung oder anderweitige, zwischenzeitlich erfolgte Einigung bezüglich des weiteren Vorgehens?

39. Ist von Seiten der Bundesregierung diesbezüglich eine Änderung des Grundgesetzes geplant, und wann will die Bundesregierung dem Parlament einen entsprechenden Vorschlag vorlegen?

40. Ist nach Ansicht der Bundesregierung ein Mandat des Deutschen Bundestages für einen digitalen Gegenschlag („Hackback“) notwendig?

    Falls nicht, wie begründet die Bundesregierung diese Rechtsauffassung?

41. Wie bewertet die Bundesregierung die Gefahr, dass durch Angriffe und das Eindringen in fremde Systeme („Hackbacks“) Eskalationsspiralen im digitalen Raum befördert werden können?

42. Hat die Bundesregierung einen multidisziplinären Prüfprozess nach Artikel 36 des Zusatzprotokolls vom 8. Juni 1977 zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte (ZP I) der Genfer Konvention für Einsätze offensiver Fähigkeiten der Bundeswehr zum Wirken im Cyber-Raum und deren Vereinbarkeit mit dem geltenden humanitären Völkerrecht durchgeführt, und wenn ja, mit welchem Ergebnis?

    Falls nein, warum nicht?

43. Sieht die Bundesregierung die Gefahr, wonach undifferenzierte, nicht näher erläuterte Angaben zu „millionenfachen Cyberangriffen“ (vgl. etwa die Zahlen aus der Antwort der Bundesregierung auf die Schriftliche Frage zur Bundeswehr, Quelle siehe Fragen 5 und 6) schon aufgrund etwa der fehlenden näheren Aufschlüsselung nach Gefahrenstufen geeignet sein können, mehr Verunsicherung statt Aufklärung der Öffentlichkeit zu bewirken, und wenn nein, warum nicht?

44. Hat die Bundesregierung eine Position zur Forderung des Inspekteurs Cyber- und Informationsraum der Bundeswehr, Generalleutnant Ludwig Leinhos nach Einrichtung eines so genannten „digitalen Verteidigungsfalles“, der unterhalb der Schwelle eines „klassischen Verteidigungsfalles“ anzusiedeln sei (vgl.: www.tah.de/welt/afp-news-single/cyber-inspekteur-brauchen-koordinator-im-nationalen-cyber-abwehrzentrum.html), und wenn ja, welche?

    a) Was genau ist nach Ansicht der Bundesregierung unter einem „digitalen Verteidigungsfall“ zu verstehen?

    b) Welche gesetzlichen Grundlagen bestehen nach Ansicht der Bundesregierung hierfür bzw. wären zu schaffen?

    c) Welche Voraussetzungen müssen erfüllt sein, dass es zur Ausrufung eines solchen „digitalen Verteidigungsfalles“ käme?

       Welche Kompetenzen und welche Rolle kämen jeweils dem Deutschen Bundestag, dem Bundesrat sowie der Bundesregierung zu?

    d) Plant die Bundesregierung hierzu Gesetzesinitiativen bzw. Änderungen des Grundgesetzes?

45. Ist aus Sicht der Bundesregierung der Übergang von der sogenannten Cyberabwehr zur „Cyberverteidigung“ ausreichend klar gesetzlich geregelt?

    Wenn nein, wo besteht hier Nachsteuerungsbedarf?

Berlin, den 25. Juni 2019

Katrin Göring-Eckardt, Dr. Anton Hofreiter und Fraktion



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333